IN THE CLAIMS

Following are the current claims. For the claims that have NOT been amended in this response, any difference between the claims below and the current state of the claims is unintentional and in the nature of a typographical error:

1. (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given [stage and] encryption/decryption context identifier, there being at least as many encryption/decryption context identifiers as the predetermined number of stages in the encryption/decryption process;

indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption context identifier; and

generating an output datablock from the source datablock and its corresponding initial variable.

2. (Original) The method of claim 1 wherein in the indexing step the bank of initial variables comprises a number of initial variables for each encryption/decryption context identifier that is at least as large as the predetermined number of stages.

3. (Original) The method of claim 1 additionally comprising the step of replacing the corresponding initial variable with the output datablock.

4. (Original) The method of claim 4 wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables.

5. (Original) The method of claim 4 wherein the encryption/decryption process comprises a block cipher capable of being pipelined.

6. (Original) The method of claim 5 wherein the process is Digital Encryption Standard (DES).

7. (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

for each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages, receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for the corresponding encryption context identifier;

for each of the plurality of encryption/decryption contexts, indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables and prior-stage output datablocks to retrieve a seed variable for the source datablock; and

for each of the plurality of encryption/decryption contexts, generating an output datablock from the source datablock and its corresponding seed variable;

wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablocks from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine.

8. (Original) The method of claim 7 wherein each of the plurality of encryption/decryption contexts comprises a telecommunications data stream to be encrypted.

9. (Original) The method of claim 8 additionally comprising the step of decrypting the output datablocks at a plurality of locations distributed from the encryption/decryption engine corresponding in number to number of encryption/decryption contexts.

10. (Original) The method of claim 7 wherein the encryption/decryption process comprises Cipher Block Chaining Mode.

11. (Original) The method of claim 10 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

12. (Currently Amended) A multi-stage pipelined encryption engine for an encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the encryption/decryption engine comprising:

means for receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given [stage and] encryption/decryption context identifier, there being at least as many encryption/decryption context identifiers as the predetermined number of stages in the encryption/decryption process;

means for indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption context identifier; and

means for generating an output datablock from the source datablock and its corresponding initial variable.

13. (Original) The encryption/decryption engine of claim 12 wherein in the indexing means the bank of initial variables comprises a number of initial variables for each encryption/decryption context identifier at least as large as the predetermined number of stages.

14. (Original) The encryption/decryption engine of claim 12 additionally comprising means for replacing the corresponding initial variable with the output datablock.

15. (Original) The encryption/decryption engine of claim 12 wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables.

16. (Original) The encryption/decryption engine of claim 15 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

17. (Currently Amended) An encryption/decryption engine for enhancing throughput of a multi-stage pipelined encryption/decryption process comprising a predetermined number of stages and providing feedback around the stages, the method comprising the steps of:

means for, as to each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages, receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for the corresponding encryption context identifier;

means for, as to each of the plurality of encryption/decryption contexts, indexing according to the encryption/decryption context identifier into a bank of variables comprising initial variables and prior-stage output datablocks to retrieve a seed variable for the source datablock; and

means for, as to each of the plurality of encryption/decryption contexts, generating an output datablock from the source datablock and its corresponding seed variable;

wherein each stage of the pipelined encryption/decryption engine at any given time is processing source datablocks from an encryption/decryption context different than encryption/decryption contexts of source datablocks being processed in all other stages of the pipelined encryption/decryption engine.

18. (Original) The encryption/decryption engine of claim 17 wherein each of the plurality of encryption/decryption contexts comprises a telecommunications data stream to be encrypted.

19. (Original) The encryption/decryption engine of claim 18 additionally comprising means for transmitting the output data blocks to be decrypted at a plurality of locations

distributed from the encryption/decryption engine corresponding in number to the number of encryption/decryption contexts.

20. (Original) The encryption/decryption engine of claim 17 wherein the encryption/decryption process comprises Cipher Block Chaining Mode.

21. (Original) The encryption/decryption engine of claim 20 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).